DEPARTMENT OF THE ARMY EC 1110-1-90
U.S. Army Corps of Engineers
CECW-EP Washington, D.C. 20314-1000

Circular
No. 1110-1-90 1 July 1998

EXPIRES 30 JUNE 2000

Engineering and Design

USE, ACQUISITION, AND SECURITY OF PRECISE POSITIONING SERVICE GPS RECEIVERS FOR CIVIL APPLICATIONS

Distribution Restriction Statement

Approved for public release; distribution is unlimited.

DEPARTMENT OF THE ARMY EC 1110-1-90
U.S. Army Corps of Engineers
CECW-EP Washington, D.C. 20314-1000

Circular
No. 1110-1-90 1 July 1998

EXPIRES 30 JUNE 2000

Engineering and Design

USE, ACQUISITION, AND SECURITY OF PRECISE POSITIONING SERVICE GPS RECEIVERS FOR CIVIL APPLICATIONS

1. Purpose. This circular disseminates policy and procedures on the use, acquisition, decryption, and security of tactical Global Positioning System (GPS) receivers for civil applications, such as the Precision Lightweight GPS Receiver (PLGR). Procedures are defined for obtaining these military grade receivers containing secure Precise Positioning Service (PPS) capabilities. This circular effects the transfer of proven military technology to civil users.

2. Applicability. This circular is applicable to USACE commands having civil works, military construction, and environmental restoration responsibilities. Personnel of the U.S. Army Corps of Engineers (USACE) are authorized to use tactical GPS receivers in the conduct of Corps civil and military construction programs.

3. References.

a. Rules for Obtaining Navstar GPS Security Devices, DOD GPS Joint Program Office, Revision A, 12 June 1997.

b. Navstar Global Positioning System Cryptographic Key Ordering Instructions, U.S. Space Command, Revision 3, June 1997.

c. EM 1110-1-1003, NAVSTAR Global Positioning System Surveying, 1 August 1996.

4. Distribution. Approved for public release. Distribution is unlimited.

5. Background. The Navigation Satellite Time and Ranging (NAVSTAR) Global Positioning System is a space-based satellite radio navigation-system developed by the U.S. Department of Defense. GPS receivers provide land, marine, and airborne users with continuous three-dimensional position, velocity, and time data (PVT). This information is available free of charge to an

unlimited number of users. The system operates under all weather conditions, 24 hours a day, anywhere on Earth. GPS provides two levels of positional accuracy: Standard Positioning Service (SPS) and Precise Positioning Service (PPS). For security reasons, DOD degrades/encrypts the GPS signals, using selective availability (SA) and anti-spoofing (AS) techniques. Any civil user can access the SPS signal with a $100 to $500 commercial grade receiver and obtain an accuracy of approximately 100 m (95%). Authorized PPS users can access and decode the encrypted P(Y)-code signal and thus obtain an approximately 10 m positional accuracy unaffected by AS and SA. Access to the PPS signal is controlled through the use of cryptographic techniques, and is limited to U.S. and allied military forces. DOD authorizes PPS access to other government and selected private sector users provided appropriate security requirements and other selection criteria are met. As a DOD component, USACE is authorized access to the tactical PPS signal for its civil works, military construction, or environmental restoration missions. The small, hand-held, PLGR receivers (AN/PSN-11R) can provide real-time, 10-meter absolute positioning or navigation accuracy, and have wide tactical use in military air/land/sea navigation, and related tactical mapping, surveying, and positioning uses. These same receivers can be used to support a variety of USACE civil functions and applications, including GIS development, natural resource management, surveying, land/air/sea navigation, and emergency management.

6. PLGR Project Applications. Stand-alone GPS receivers can compute and display "absolute" geographic positions in real-time throughout most of the world. Absolute GPS positioning is distinguished from differential GPS (DGPS) positioning which requires a simultaneous comparison of positions between two nearby GPS receivers; typically using a communications data link between the two receivers. Accuracies of code-phase DGPS range between 0.5 and 10 m. DGPS carrier-phase differencing techniques can provide relative positional accuracies at the millimeter level. Project functional accuracy requirements and economics will determine whether absolute (either SPS or PPS) or differential GPS techniques are required. PPS accuracies at the 10 meter level will yield sufficient accuracy for many environmental, GIS, and project management applications. PLGR receivers represent an economical navigation and positioning tool compared to traditional surveying or differential GPS methods. In general, PLGR accuracies are suitable for GIS mapping scales of 1:12,000 (1" = 1000 ft) or smaller. PLGR accuracies may also have application in dredge/scow positioning or monitoring,

environmental mapping, vehicle navigation, and emergency management operations. Where only 100 meter accuracy is required, less-expensive SPS receivers should be used. For accuracies exceeding 10 meters, differential GPS techniques are necessary. All GPS receivers can be operated with minimal training.

a. Current USACE Applications. The use of a PLGR receiver could be applicable whenever the mission requires positioning accuracies that are better than the 100 meters obtained by an SPS receiver, but do not require the specialized equipment needed to acquire differential GPS accuracies. Some of the applications where the use of a PLGR receiver has proven to be effective include emergency management, real estate, OCONUS control surveys, archeological surveys, GIS data collection, wetland delineation, and Corps regulatory activities.

b. Training Options. In order to obtain maximum efficiency from the operation of a GPS receiver, either PPS or SPS, the user must be trained in the operation of the receiver and the receiver interface with ancillary equipment. Training options exist within USACE (U.S. Army Topographic Engineering Center), other government agencies, and the private sector.

7. <u>Acquisition of PPS Receivers</u>. Outlined below are two procurement options available to USACE commands to obtain PPS receivers.

a. PLGR/SOLGR PPS Receivers. USACE users can purchase the PLGR receivers using a Department of Agriculture (USDA) multi-agency contract. The cost in 1998 for a PLGR with a complete complement of accessories (PLGR Kit) is $2,091.00. Although the USDA contract will expire in 1998, the USDA is currently working toward establishing an amendment to the existing contract or a new contract for delivery of PPS receivers starting in January 1999. The receiver that will probably be delivered in 1999 and beyond will be termed the Special Operations Lightweight GPS Receiver, or SOLGR. This receiver will offer several improvements over the PLGR such as 12 channels, dual frequency operation, waterproof down to 24 meters, programmable function keys.

(1) PLGR/SOLGR Receiver Description. These hand-held PPS receivers are manufactured by Rockwell Incorporated, Collins Avionics Division. The PLGR and SOLGR will determine positions to an accuracy of 16 meters SEP when operating in the PPS mode

and 100 meters when operating in the SPS mode. Additionally, both instruments contain Wide Area GPS Enhancement (WAGE) for autonomous positioning accuracy to 4 meters CEP and Secure (Y-code) Differential GPS (SDGPS) for positioning accuracy to less than 2 meters CEP. Many vendors interface with the PLGR and SOLGR for GIS applications.

(2) Acquisition Procedures. To procure the PLGR or SOLGR from the USDA contract, first contact the U.S. Army Topographic Engineering Center (USATEC), Geospatial Engineering Branch, ATTN: CETEC-TD-G, 7701 Telegraph Road, Alexandria, VA 22315-3864, telephone (703) 428-6798, e-mail: <pcervari@tec.army.mil>, and request an order form. Complete the form, prepare the paperwork (MIPR, credit card, etc.) to cover cost of required equipment, and fax to USATEC (703-428-6135). USATEC will place the order with the vendor, receive and load the cryptographic keys, check the equipment to insure proper operation, and Fed-Ex the hardware to the ordering office.

b. Non-PLGR/SOLGR PPS Receivers. USACE users can also purchase any other PPS receivers directly from the manufacturer. These receivers can be purchased using standard competitive procurement practices.

(1) Procedure. Approval to purchase a PPS receiver directly from the manufacturer must first be obtained by submitting correspondence to the GPS Joint Program Office (JPO), Headquarters Space and Missile Systems Center, ATTN: CZU, Los Angeles AFB, 2435 Vela Way, El Segundo, CA 90245-5500, defining the project that requires more precise positioning than can be obtained using SPS receivers. The correspondence received from GPS JPO will authorize direct negotiations with the vendor(s).

8. Cryptographic Key Control and Use.

a. General Discussion. PPS requires receivers be loaded with a cryptographic code so that the effects of Selective-Availability (SA) are negated, and to provide for Anti-Spoofing (A-S) capability. To receive the cryptographic keys requires a COMSEC custodian and to load the key into the GPS receiver requires a COMSEC fill device.

b. Acquiring COMSEC Keys. To obtain the cryptographic keys, the COMSEC custodian must process a request for keying material through the Validating Authority for the U.S Army, the Communications Security Logistics Agency (CSLA), ATTN: SELCL-KP-

KEY, Ft. Huachuca, AZ 85613-7090, who validates the operational need for PPS accuracies and forwards the request to the GPS Controlling Authority. The Deputy Undersecretary of Defense Space (ODUSD/C3I) has designated HQ U.S. Space Command as the Controlling Authority for PPS cryptographic keying material, who, in turn, will notify the appropriate Distribution Center to make distribution to the identified COMSEC Custodian. The actual cryptographic keys are classified CONFIDENTIAL and must be handled accordingly. A keyed receiver is not classified but must be safeguarded like any valuable piece of equipment. If an annual key is not compromised and there are no accidental “zeroizations” of the keyed receiver, the receiver need only be keyed once per key-year.

c. Loading the PPS Receiver. There are several ways the user can have his PPS receiver loaded with the necessary COMSEC key.

(1) District/Division COMSEC Custodian. If the District or Division Office has a COMSEC Custodian, and the COMSEC Custodian has processed and obtained the yearly COMSEC key and the fill devices, each year the PPS receiver will need to be taken to the COMSEC Custodian to have the new key loaded into the receiver. Note: If the receiver is not re-keyed, it will continue to operate, but will operate only as an SPS receiver until re-keyed.

(2) U.S. Army Topographic Engineering Center. Those Districts and Divisions that do not have a COMSEC Custodian may Fed-Ex the receiver(s) overnight to the U.S. Army Topographic Engineering Center, 7701 Telegraph Road, ATTN: CETEC-TD-G, Alexandria, VA 22315-3864. Enclosed with the receiver(s) to be re-keyed should be a completed return Fed-Ex shipping document. CETEC will replace the memory battery, check PPS operation and return the receiver(s).

(3) Other Military Offices. For those USACE commands who do not have a COMSEC Custodian but have a military installation close to their office, the military installation may have a COMSEC Custodian, the COMSEC keys, and the fill devices. The military office may be willing to re-key the PPS receivers. The USACE command should contact the military installation to determine if this approach is feasible.

9. <u>Proponency and Technical Support</u>. The HQUSACE proponent for this circular is Engineering Division, Directorate of Civil Works, ATTN: CECW-EP. Technical assistance on security requirements or the acquisition of PPS receivers may be obtained from the Geospatial Engineering Branch, U.S. Army Topographic Engineering Center, ATTN: CETEC-TD-G, 7701 Telegraph Road, Alexandria, VA 22315-3864, (703) 428-6798, e-mail: <pcervari@tec.army.mil>.

FOR THE COMMANDER:

ROBERT W. BURKHARDT
Colonel, Corps of Engineers
Executive Director of Civil Works

1 Appendix
APP A - Additional
Information on GPS

APPENDIX A
Additional Information on GPS

A-1. Components of GPS. The GPS system consists of three major segments: the space segment, the control segment and the user segment.

a. Space Segment. The Space Segment consists of a nominal constellation of 24 operational satellites (including 3 spares) which have been placed in 6 orbital planes 10,900 miles (20,200 km) above the Earth's surface. The satellites are in circular orbits with a 12-hour orbital period and inclination angle of 55 degrees. This orientation nearly ensures a minimum of five satellites in view at any given time, anywhere on Earth. Each satellite continuously broadcasts two low-power spread-spectrum RE Link signals (L1 and L2). The L1 signal is centered at 1575.42 MHZ and the L2 signal is centered at 1227.6 MHZ.

b. Control Segment. The Control Segment consists of a Master Control Station (in Colorado Springs), and a number of monitor stations at various locations around the world. Each monitor station tracks all the GPS satellites in view and passes the signal measurement data back to the Master Control Station, where the computations are performed to determine precise satellite ephemeris and satellite clock errors. This data is then up linked to the individual satellites, and subsequently rebroadcast by the satellite as part of its navigation data message.

c. User Segment. The User Segment is the collection of all GPS receivers and their application support equipment such as antennas and processors. This equipment allows users to receive, decode, and process the information necessary to obtain accurate position, velocity, and timing measurements. This data is used by the receiver's support equipment for specific application requirements.

A-2. Characteristics of GPS Signals. The satellites transmit their signals using spread spectrum techniques employing two different spreading functions: a 1.023 MHZ coarse/acquisition (C/A) code on L1 only and a 10.23 MHZ precision (P) code on both L1 and L2. The two spreading techniques provide two levels of GPS service: Precise Positioning Service (PPS) and Standard Positioning Service (SPS). SPS uses C/A code to derive position, while PPS uses the more precise P(Y)-code.

(1) The P-code has a number of advantages over C/A code. First, the chipping rate of the P-code is 10 times faster, therefore the wavelength is 1/10th as long, giving the P-code a much higher resolution. Second, the higher chipping rate spreads the signal over a wider frequency range that makes the P-code much more difficult to jam. Third, by encrypting the P-code (creating the Y-code), the receiver is not susceptible to spoofing, or false GPS signals intended to deceive the receiver.

(2) The drawback of P-code is that it is relatively difficult to acquire because of its length and high speed. For this reason, many PPS receivers first acquire C/A code, then switch over to the P(Y)-code.

(3) Y code is an encrypted version of P code, used for anti-spoofing (A-S). Due to the similarity of these two codes, they are referred to collectively as P(Y)-code.

(4) Superimposed on both the P-code and the C/A code is a navigation message (NAV-msg) containing satellite ephemeris data, atmospheric propagation correction data, satellite clock-bias information, and almanac information for all satellites in the constellation.

(5) The GPS satellites use Bi-Phase Shift Keyed (BPSK) modulation to transmit the C/A and P(Y)-codes. The BPSK technique involves reversal of the carrier phase whenever the C/A or P(Y)-code transitions from 0 to 1 or from 1 to 0.

(6) To the casual observer, the very long sequence of ones and zeros that make up the C/A and P-codes would appear to occur in a random fashion and blend into the background noise. For this reason, they are known as pseudo-random noise (PRN). In actuality, the C/A and P-codes generated are precisely predictable to the start time of the code sequence and can be duplicated by the GPS receiver. The amount the receiver must offset its code generator to match the incoming code from the satellite is directly proportional to the range between the GPS receiver antenna and the satellite.

(7) By the time the spread spectrum signal arrives at the GPS receiver, its signal power is well below the thermal noise level. To recover the signal, the receiver uses a correlation method to compare the incoming signals with its own generated C/A or P(Y) codes. The receiver shifts its generated code until the two codes are correlated.

A-3. <u>Determining Positions</u>.

a. The receiver continuously determines its geographic position by measuring the ranges (the distance between a satellite with known coordinates in space and the receiver*s antenna) of several satellites and computes the geometric intersection of these ranges.

b. To determine a range, the receiver measures the time required for the GPS signal to travel from the satellite to the receiver antenna. The resulting time shift is multiplied by the speed of light, arriving at the range measurement.

c. Since the resulting range measurement contains propagation delays due to atmospheric effects, as well as satellite and receiver clock errors, it is referred to as a “pseudorange.” A minimum of four pseudorange measurements is required by the receiver to mathematically determine time and the three components of position (latitude, longitude, and elevation). The solution of these equations may be visualized as the geometric intersection of four ranges from four known satellite locations.

d. If one of the variables is known, such as elevation, only three satellite pseudorange measurements are required for a PVT solution, and only three satellites would need to be tracked.

A-4. <u>GPS Error Budgets and Accuracies</u>.

a. GPS accuracy has a statistical distribution that is dependent on a number of important factors, including: dilution of precision (DOP) satellite position and clock errors, atmospheric delay of satellite signals, selective availability, signal obstruction, and multipath errors.

b. Each satellite follows a known orbit around the earth and contains a precise atomic clock. The monitor stations closely track each satellite to detect any errors in its orbits or clock. Corrections for errors are sent to each satellite as ephemeris and almanac data. The ephemeris data contains specific position and clock correction data for each satellite while the almanac contains satellite position data for all satellites. The NAV set receives the ephemeris and almanac data from the satellites and uses this data to compensate for the position and clock errors when calculating the NAV data.

c. There are two ways to compensate for the atmospheric delays: modeling and direct measurement. The ionospheric and tropospheric delays are inversely proportional to the square of the frequency. If a receiver can receive L1 and L2 frequencies, it can measure the difference between the two signals and calculate the exact atmospheric delay.

d. Currently, most receivers use mathematical models to approximate the atmospheric delay. The tropospheric effects are fairly static and predictable and a model has been developed that effectively removes 92-95 percent of the error.

e. The ionosphere is more difficult to model due to its unusual shape and the number of factors that affect it. Therefore, a model has been developed that requires eight variable coefficients. Every day, the Control Segment calculates the coefficients for the ionospheric model and uplinks them to the satellites. The data is then rebroadcast in the NAV messages of the C/A- and P(Y)-codes. This model can effectively remove 55 percent of the ionospheric delay.

f. Multipath errors result from the combination of data from more than one propagation path. This distorts the signal characteristics from which the range measurements are made, resulting in pseudorange errors. These errors are dependent on the nature and location of a reflective surface peculiar to each user location. The effects are less detrimental for a moving user since small antenna movement can completely change the multipath characteristics.

g. The receiver is designed to reject multipath signals. First, the active patch antennas are designed to have a sharp gain roll-off near the horizon while providing nominal gain for the primary satellite signal. Since most multipath signals are reflected from ground structures, they tend to be attenuated. Second, the antenna is right-hand polarized. When a right-hand polarized GPS signal is reflected off a conductive surface, it becomes left-hand polarized, and rejected by the antenna. The receiver also has hardware and software designed to reduce the effects of any multipath interference errors.

A-5. GPS Positioning Services. GPS satellites provide two levels of navigation service: Standard Position Service (SPS) and Precise Position Service (PPS).

(1) SPS receivers use GPS information broadcast in the clear and is available to anyone in the world. This information contains built-in errors that limit the accuracy of the receiver. This is a security technique called Selective Availability (SA). These SA errors are variable. In normal conditions, the U.S. government guarantees that these errors do not exceed 100 meters horizontal, 140 meters vertical, and time accuracy of 340 nanoseconds 95 percent of the time. Thus, there are times when an SPS receiver error exceeds these limits. SA is always on. SPS receivers are for civil use and a PLGR without crypto keys will act like an SPS receiver.

(2) PPS receivers use the same information as SPS receivers. They also read encoded information that contains the corrections to remove the intentional SA errors. Only users who have crypto keys to decode this information get the PPS accuracy. U.S. government agencies and some Allies are authorized to have these crypto keys. A PLGR with valid crypto keys loaded and verified is a PPS receiver.

(3) To protect authorized users from hostile attempts to imitate the GPS signals, a security technique called Anti-spoofing (A-S) is also used. This is an encrypted signal from the satellites that can only be read by PPS receivers. A receiver with valid crypto keys loaded and verified, reads this encrypted signal and operates in a spoofing environment.

(4) Normal operation of the GPS receiver requires undisturbed reception of signals from as few as four satellites (in normal 3-D mode) or three satellites in fixed-elevation mode. The signals propagating from the satellites cannot penetrate water, soil, walls, or other similar obstacles. The antenna and the satellites are required to be in a "line-of-sight" with each other. Therefore, GPS cannot be used for underground positioning in tunnels, mines, or subsurface marine navigation. In surface navigation, the signal can be obscured by buildings, bridges, and other matter that might block an antenna*s line-of-sight from the GPS satellites in view. In airborne applications, the signal can be shaded by the aircraft*s body during high banking angles.

A-6. <u>Differential GPS (DGPS)</u>. Differential GPS (DGPS) may be used to eliminate the effects of SA and correct certain bias-like errors in the GPS signals. A Reference Station receiver measures ranges from all visible satellites to its surveyed position. Differences between the measured and known ranges are computed and applied to differential equipped receivers in a local area.

These differences (or Pseudo-Range Corrections) can be transmitted by radio and applied in real-time, or can be downloaded into computer software and applied during postprocessing.